Segurança da Informação em Foco: Análise Curricular dos Cursos de Computação da Rede Federal no Sudeste do Brasil

Bruno Raphael Andrade Varjão Meireles[1], **Lídia Bononi Paiva Tomaz**[1]

[1]Instituto Federal do Triângulo Mineiro (IFTM)
Uberaba – MG – Brasil

bruno.meireles@estudante.iftm.edu.br, lidia@iftm.edu.br

Abstract. *In computing programs, the topic of Information Security is essential given the growing increase in cyber threats. In this context, this study investigated the presence of this topic in the curricula of courses offered by the Federal Network of Professional, Scientific, and Technological Education in Southeast Brazil, through the analysis of Pedagogical Course Projects (PCPs) of bachelor's, technology, and licentiate programs. The results showed that the topic is significantly present in bachelor's and technology courses but remains limited in computing licentiate programs. Nevertheless, the need to strengthen the inclusion of this theme in curricula is evident, aiming to align academic training with contemporary demands in cybersecurity.*

Resumo. *Nos cursos de computação, o tema de Segurança da Informação é essencial diante do crescente aumento das ameaças cibernéticas. Neste contexto, este estudo investigou a presença dessa temática nos currículos de cursos da Rede Federal de Educação Profissional, Científica e Tecnológica no Sudeste do Brasil, por meio da análise de Projetos Pedagógicos de Curso de bacharelados, tecnólogos e licenciaturas. Os resultados mostraram que o tema está presente de forma significativa em bacharelados e tecnólogos, mas é escasso nas licenciaturas em Computação. Apesar disso, observa-se a necessidade de fortalecer a inserção dessa temática nos currículos, visando alinhar a formação acadêmica às demandas contemporâneas de segurança cibernética.*

1. Introdução

O aumento das ameaças cibernéticas e das violações de dados expõe fragilidades nos sistemas digitais, comprometendo a privacidade dos cidadãos e a segurança das organizações. No Brasil, de acordo com dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança, apenas no ano de 2024, foram registradas mais de 500 mil notificações de incidentes cibernéticos [CERT.br 2025]. Esse tipo de evento vem impactando não apenas entidades privadas [CISO Advisor 2024a, O Globo 2023], mas também órgãos públicos [Ministério da Saúde 2022] e instituições educacionais [G1 Mato Grosso do Sul 2023, CISO Advisor 2024b, Security Leaders 2024, UFRGS 2024]. Tal situação evidencia a amplitude e a gravidade do problema.

Esse elevado número de incidentes está diretamente relacionado ao avanço da transformação digital, que inclui o desenvolvimento acelerado de aplicações baseadas na web, o aumento significativo do uso de dispositivos da Internet das Coisas (IoT), a popularização da computação em nuvem e a consolidação do modelo de trabalho remoto,

intensificado pela pandemia e mantido na atualidade [IBM Security 2023]. Esse cenário contribui para a ampliação da superfície de ataque, uma vez que mais dispositivos e sistemas passam a ser conectados, criando novos pontos de vulnerabilidade e aumentando os riscos de exploração por agentes mal-intencionados [Almohri et al. 2020].

Neste contexto, organizações, governos e especialistas têm se mobilizado para desenvolver *frameworks*, programas e boas práticas para orientar a adoção de medidas preventivas e mitigatórias para a Segurança da Informação. Destacam-se, nesse cenário, as recomendações do *National Institute of Standards and Technology* [NIST 2024], por meio do *NIST Cybersecurity Framework* (NIST CSF) e os Controles Críticos de Segurança do *Center for Internet Security* [CIS 2025], denominados *CIS Controls*. Além disso, o Governo Federal do Brasil reconheceu a urgência do tema ao instituir, em 2023, o Programa de Privacidade e Segurança da Informação (PPSI) visando o fortalecimento da segurança da informação no âmbito da Administração Pública Federal [BRASIL 2023].

Estes *frameworks* e diretrizes explicitam a necessidade dos princípios de *Security by Design*, que preconizam que a segurança seja considerada desde o início do ciclo de vida de qualquer projeto ou sistema digital[Bygrave 2022]. Essa segurança contempla desde medidas técnicas, até medidas administrativas que assegurem a proteção de dados contra acessos não autorizados. Nesse contexto, torna-se fundamental refletir sobre o papel da formação acadêmica na capacitação dos futuros profissionais de Tecnologia da Informação (TI) quanto às práticas de segurança desde a concepção dos sistemas. Estudos apontam que a insuficiência de conhecimento técnico sobre esses princípios nas organizações está entre as principais causas da recorrência de incidentes cibernéticos [Cristani et al. 2020, Souza et al. 2020, de Barros 2023, Lopes 2023].

Diante disso, o presente trabalho propõe analisar a abordagem da temática da Segurança da Informação nos currículos dos cursos de bacharelado, licenciatura e tecnólogos da área de computação, ofertados por instituições da Rede Federal de Educação Profissional, Científica e Tecnológica (RFEPCT) da Região Sudeste do Brasil. A escolha desta região justifica-se pela expressiva concentração de instituições de ensino, empresas e polos tecnológicos, o que potencializa a demanda por profissionais qualificados para enfrentar os desafios impostos pelo cenário digital atual.

A principal contribuição deste trabalho é indicar se os cursos de computação de instituições da RFEPCT consideram o tema de Segurança da Informação em suas matrizes curriculares. Assim, espera-se contribuir para a reflexão sobre como este tema está inserido nos currículos, oferecendo subsídios para que instituições de ensino aprimorem as suas ofertas de cursos visando a preparação dos profissionais frente às exigências normativas e aos riscos do mundo digital. Os resultados obtidos demonstram que a temática da Segurança da Informação está presente de forma significativa nas matrizes curriculares dos cursos analisados. No entanto, a análise revelou diferenças importantes entre as modalidades de curso, com destaque para a baixa inserção da temática nas licenciaturas.

Este trabalho está organizado da seguinte forma: a Seção 2 apresenta os trabalhos correlatos; a Seção 3 detalha a metodologia adotada; a Seção 4 expõe os resultados e discussões; e, por fim, a Seção 5 apresenta as conclusões e trabalhos futuros.

2. Trabalhos Correlatos

Diversos estudos destacam a importância da segurança cibernética na educação e sua presença nos currículos acadêmicos. [Cristani et al. 2020] investigaram a inclusão da disciplina de Segurança da Informação nos cursos de Sistemas de Informação no Brasil, identificando que, embora 92% dos cursos abordem o tema, a carga horária não se traduz necessariamente em maior domínio do conteúdo pelos alunos, evidenciando a necessidade de aprofundamento na qualidade do ensino.

De forma semelhante, [de Barros 2023] analisou a educação em segurança cibernética em escolas e universidades brasileiras, ressaltando a importância da conscientização acadêmica na mitigação de incidentes. Nesta linha, [Lopes 2023] aponta que países com programas estruturados na área registram menor incidência de vulnerabilidades digitais, reforçando a relevância de um ensino bem fundamentado.

Além disso, [Souza et al. 2020] abordaram a governança da segurança da informação em instituições públicas de ensino superior, evidenciando lacunas na capacitação de usuários e na gestão de processos de segurança. Ainda, [Abu-Taieh 2017] analisou currículos internacionais de mestrados em segurança cibernética, identificando grande variação na estrutura curricular e a ausência de um padrão global, o que ressalta a necessidade de diretrizes mais homogêneas na formação acadêmica.

3. Metodologia

Este trabalho caracteriza-se como uma pesquisa de natureza primária, de caráter exploratório, com procedimento de análise documental [Wazlawick 2020]. A pesquisa é classificada como primária, pois gera conhecimento original por meio da análise de documentos institucionais como os Projetos Pedagógicos de Curso (PPCs). O caráter exploratório da pesquisa reside na investigação aberta do fenômeno, buscando levantar aspectos que subsidiem a reflexão sobre a presença dessa temática na formação acadêmica. Como procedimento técnico, adota-se a análise documental, uma vez que o estudo se fundamenta no exame de matrizes curriculares e ementas disponibilizadas em documentos oficiais pelas instituições de ensino selecionadas.

A definição dos cursos analisados considerou o levantamento das formações da área de Computação previstas nas Diretrizes Curriculares Nacionais para os cursos de graduação na área da Computação [Ministério da Educação 2016], bem como no Catálogo Nacional de Cursos Superiores de Tecnologia, com foco no eixo tecnológico de Informação e Comunicação [Ministério da Educação 2025]. Foram selecionadas instituições da RFEPCT da Região Sudeste do Brasil, conforme a Lei nº 11.892/2008. A inclusão considerou a localização da reitoria, abrangendo Institutos Federais (IFs) e Centros Federais de Educação Tecnológica (CEFETs).

Após essa delimitação, foram mapeados todos os cursos da área de computação ofertados pelas instituições selecionadas, considerando as ofertas em cada um de seus campi. Em seguida, foram identificados e analisados os PPCs correspondentes, com o objetivo de examinar suas matrizes curriculares e as ementas das unidades curriculares (UCs). Para isso, foi realizada uma busca textual nos documentos pelo termo “segurança”. O objetivo foi identificar as UCs que contêm esse termo em seu nome, bem como aquelas que, apesar de não o incluírem no título, abordam a temática de segurança em suas

ementas. Os dados obtidos foram tabulados de forma sistemática, permitindo uma análise descritiva. A Tabela 1 apresenta o dicionário de dados construído para orientar a coleta das informações durante o levantamento.

ID	Nome do atributo	Valores
1	Nome da Instituição	Centro Federal de Educação Tecnológica de Minas Gerais (CEFET-MG) Centro Federal de Educação Tecnológica do Rio de Janeiro (CEFET-RJ) Colégio Pedro II Instituto Federal do Espírito Santo (IFES) Instituto Federal Fluminense (IFF) Instituto Federal de Minas Gerais (IFMG) Instituto Federal do Norte de Minas Gerais (IFNMG) Instituto Federal do Rio de Janeiro (IFRJ) Instituto Federal de São Paulo (IFSP) Instituto Federal do Sudeste de Minas Gerais (IF Sudeste MG) Instituto Federal do Sul de Minas Gerais (IFSULDEMINAS) Instituto Federal do Triângulo Mineiro (IFTM)
2	Tipo de graduação	Bacharelado Licenciatura Tecnólogo
3	Curso	Bacharelado em Ciência da Computação Bacharelado em Engenharia de Computação Bacharelado em Engenharia de Software Bacharelado em Engenharia de Telecomunicações Bacharelado em Sistemas de Informação Licenciatura em Computação Licenciatura em Informática Tecnologia em Análise e Desenvolvimento de Sistemas Tecnologia em Gestão da Tecnologia da Informação Tecnologia em Jogos Digitais Tecnologia em Redes de Computadores Tecnologia em Sistemas de Telecomunicações Tecnologia em Sistemas para Internet
4	Ocorrência de UC com o termo “segurança” em seu nome	Sim | Não
5	Tipo da UC	Obrigatória | Optativa
6	Ocorrência do termo “segurança” na ementa de outras UCs caso o retorno do ID 4 seja igual a não	Sim | Não

Tabela 1. Dicionário de atributos da pesquisa

Optou-se por adotar uma abordagem descritiva na análise dos dados, considerando que o principal objetivo da pesquisa é apresentar um panorama sobre a inserção da temática da Segurança da Informação nas matrizes curriculares dos cursos de computação analisados. Conforme destaca [Marconi and Lakatos 2003], a análise descritiva possibilita observar, registrar e descrever os fatos sem a interferência do pesquisador, o que se mostra adequado ao propósito deste estudo de sistematizar as informações extraídas dos documentos oficiais das instituições, oferecendo um retrato fiel da realidade observada.

Cabe ressaltar que não foi realizada uma análise qualitativa para avaliar a abrangência e a profundidade com que os tópicos relacionados à Segurança da Informação

são explorados nas ementas. Por outro lado, a estratégia metodológica adotada permitiu mapear a incidência da temática, verificando se o termo "segurança" é contemplado nas UCs, ainda que de forma mínima, nos cursos analisados. Os resultados obtidos neste processo serão apresentados na Seção 4.

4. Resultados

Esta seção apresenta os resultados e a discussão referentes ao levantamento dos cursos da área de computação ofertados pela RFEPCT da Região Sudeste do Brasil. A Tabela 2 apresenta uma visão geral das ofertas por instituição. Ao todo, foram analisadas 11 instituições, sendo nove IFs e dois CEFETs. Conforme apresentado, a RFEPCT na região concentra 92 cursos na área de Computação, distribuídos em 46 bacharelados, quatro licenciaturas e 42 cursos superiores de tecnologia.

Sigla	Bacharelado	Licenciatura	Tecnólogo	Total
CEFET-MG	5	0	0	5
CEFET-RJ	5	0	0	5
IFES	3	1	4	8
IFF	4	0	1	5
IFMG	5	0	0	5
IFNMG	6	0	4	10
IFRJ	1	1	2	4
IFSP	9	0	21	30
IF Sudeste MG	2	0	4	6
IFSULDEMINAS	4	0	1	5
IFTM	2	2	5	9
TOTAL	**46**	**4**	**42**	**92**

Tabela 2. Levantamento por instituições da RFEPCT da Região Sudeste do Brasil e a distribuição dos cursos da área de computação, por modalidade

De fato, o expressivo número de cursos da área de Computação na Região Sudeste evidencia a forte demanda por profissionais do setor, impulsionada pela concentração de empresas e polos tecnológicos na região. Para detalhar a análise sobre a inserção da temática da Segurança da Informação nesses cursos, os resultados serão apresentados em três seções específicas: a Seção 4.1 traz uma visão geral das instituições e da oferta de cursos; a Seção 4.2 expõe a análise por modalidade de curso; e, por fim, a Seção 4.3 apresenta o ranqueamento das UCs mais recorrentes relacionadas à temática de segurança nos cursos analisados.

4.1. Visão geral das instituições

A Figura 1 ilustra o panorama geral da presença de UCs que abordam o tema Segurança da Informação diretamente em seu nome nas matrizes curriculares dos PPCs. Os dados revelam que 76,1% dos cursos possuem pelo menos uma UC com o termo segurança explicitamente em seu título, enquanto 23,9% não contemplam o tema de forma nominal.

Por outro lado, a Figura 2 apresenta um cenário que considera a possibilidade de o tema ser tratado em outras UCs, ainda que não mencionado no nome. Entre os cursos que não possuem UCs com o termo "segurança" no nome, 81,8% abordam o tema nas ementas de outras disciplinas. Apenas 18,2% dos cursos não apresentam o assunto em nenhum componente curricular, o que evidencia a relevância da temática, mesmo que de forma transversal.

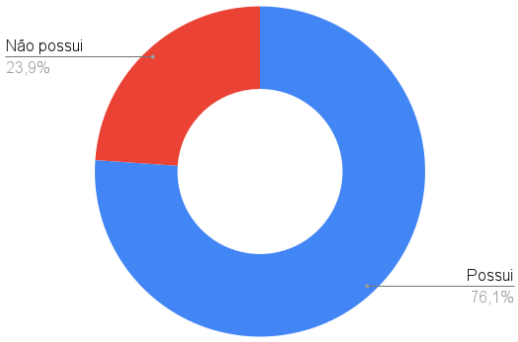

Figura 1. Cursos que contemplam o termo "segurança" na matriz curricular

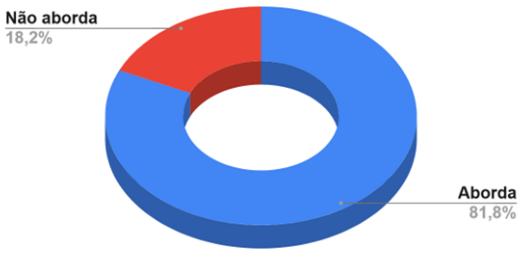

Figura 2. Cursos que abordam o tema "segurança" em outras ementas de UCs

Uma análise complementar, foi verificar o caráter da oferta quanto à obrigatoriedade das UCs entre o grupo que contempla o termo "segurança" no título da UC. A Figura 3 apresenta os resultados dessa análise. Observa-se que a maioria das UCs está inserida na matriz curricular obrigatória dos cursos, representando 88,6% do total (62 UCs). Por outro lado, apenas 11,4% (8 UCs) são ofertadas como disciplinas optativas, o que pode limitar o acesso dos estudantes ao tema, uma vez que sua abordagem dependerá das escolhas individuais ao longo do itinerário formativo.

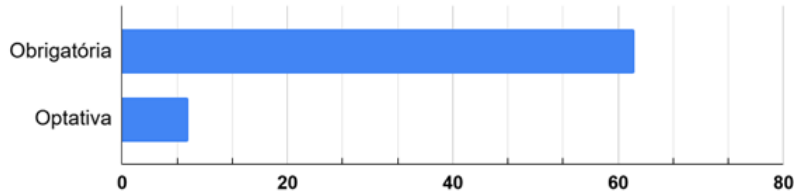

Figura 3. Tipo de oferta das UCs que possuem o termo segurança em seu nome

Estes resultados evidenciam uma presença significativa da temática "segurança" nos cursos de computação analisados. Contudo, embora a abordagem transversal do tema seja relevante, a ausência da nomenclatura "segurança" no título das UCs pode diminuir a visibilidade e a ênfase atribuída à temática ao longo da formação dos estudantes. É importante destacar que não foi realizada uma análise qualitativa das ementas, de modo que a ausência do termo no título da disciplina não implica, necessariamente, na inexistência da abordagem do conteúdo. Essa constatação é corroborada pelos dados apresentados na Figura 2.

4.2. Análise por modalidade de cursos

Esta seção apresenta a análise realizada por modalidade de cursos: bacharelado, licenciatura e tecnólogos. Os dados obtidos são apresentados na Figura 4.

A Figura 4(A) apresenta o panorama dos cursos de bacharelado, nos quais se observa que todas as ofertas contemplam a temática da Segurança da Informação em seus PPCs. Desses, 67,4% possuem ao menos uma UC que explicita o termo "segurança" no nome, enquanto 32,6% abordam o tema nas ementas de outras UCs.

Os cursos de licenciatura, conforme a Figura 4(B), apresentam uma realidade distinta. Não foi identificada nenhuma oferta que possua UCs com o termo "segurança" em

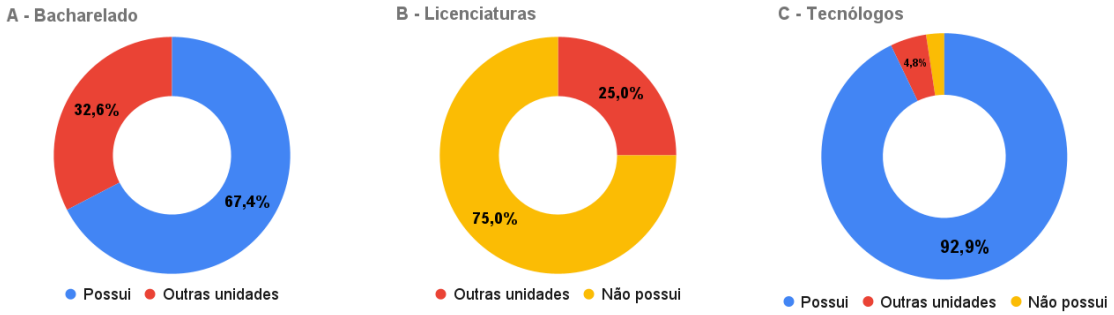

Figura 4. Visão geral por modalidade de curso de graduação (Bacharelado, Licenciatura ou Tecnólogo) sobre a oferta de UCs relacionadas ao tema de segurança da informação

seu nome. Apenas 25% dos cursos abordam o tema de maneira indireta nas ementas de outras UCs, enquanto 75% não apresentam qualquer menção ao tema em seus PPCs.

No caso dos cursos tecnólogos, ilustrados na Figura 4(C), a cobertura da temática também é expressiva. Do total de cursos analisados, 92,9% possuem UCs que apresentam o termo "segurança" no nome, 4,8% abordam o tema de forma indireta em outras UCs e apenas 2,3% não contemplam o tema de maneira alguma no PPC.

Estes resultados evidenciam um cenário de maior atenção à temática da Segurança da Informação nos cursos de bacharelado e tecnologia, o que pode estar relacionado à natureza mais técnica e prática dessas formações. Ambas as modalidades de curso demonstram uma preocupação em estruturar a abordagem do tema de forma explícita, principalmente no nome das UCs. Em contrapartida, a baixa presença do tema nos cursos de licenciatura indica uma lacuna significativa na formação dos futuros professores de computação, justamente em um período em que questões relacionadas à segurança da informação tornam-se cada vez mais relevantes no contexto educacional e social. A ausência do tema pode impactar diretamente na capacidade desses profissionais de transmitir aos seus futuros alunos a importância da segurança da informação, tanto no uso das tecnologias quanto na formação cidadã crítica e consciente.

4.3. Ranqueamento das unidades curriculares

Esta seção apresenta o ranqueamento dos nomes das UCs relacionadas à temática da Segurança da Informação que são mais frequentes nos PPCs dos cursos analisados. A Figura 5 apresenta as 10 disciplinas mais recorrentes, considerando a soma das ofertas obrigatórias e optativas.

Conforme é possível observar, o termo "Segurança da Informação" destacou-se como o mais utilizado, presente 31 vezes. Esse dado evidencia a consolidação dessa nomenclatura como padrão para abordar o tema nas formações da área de Computação. Em seguida, aparecem as UCs "Segurança de Sistemas" (12 ocorrências), "Segurança e Auditoria de Sistemas" (8 ocorrências) e "Segurança de Redes" (6 ocorrências), indicando uma preocupação complementar com aspectos técnicos e de auditoria associados à segurança.

Os resultados evidenciam uma tendência para uma abordagem generalista, refletida na predominância do título "Segurança da Informação". Tal escolha, embora positiva por garantir a presença do tema na formação, pode indicar uma certa limitação em aprofundar tópicos mais técnicos ou especializados como criptografia, segurança cibernética

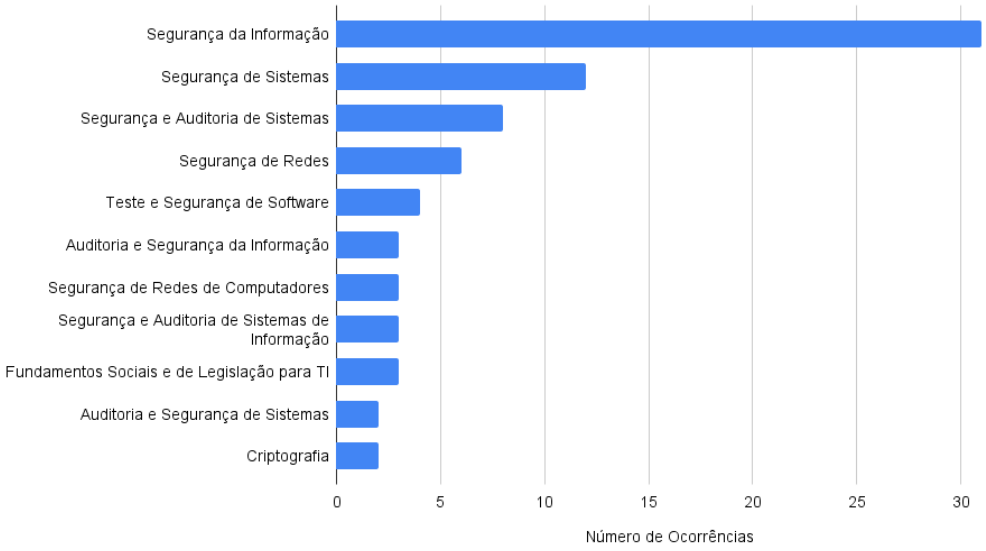

Figura 5. Top 10 das UCs que mais apareceram nas ofertas dos PPCs analisados

ou desenvolvimento de software seguro considerando os conceitos *security by design*.

Outro ponto relevante é a presença de termos ligados à auditoria e à legislação, o que sugere uma preocupação com aspectos normativos e regulatórios, alinhados às demandas atuais do mercado e à vigência da Lei Geral de Proteção de Dados. Por outro lado, a baixa ocorrência de disciplinas como "Segurança Cibernética" e "Segurança Computacional" aponta para uma oportunidade de atualização das nomenclaturas e conteúdos curriculares, considerando o avanço das ameaças digitais e a necessidade de formação de profissionais capazes de atuar em cenários mais complexos.

Essa observação, baseada na análise nominal das disciplinas, indica uma oportunidade para os cursos irem além dos aspectos gerais. Uma formação alinhada às demandas contemporâneas poderia, por exemplo, incorporar de forma mais clara a exploração de frameworks consolidados na área, como o NIST CSF e os CIS Controls, além de diretrizes estratégicas do governo, como o PPSI. Sem uma análise qualitativa das ementas, não é possível afirmar que tais tópicos estão ausentes, mas a análise aqui apresentada aponta para a necessidade de os cursos avaliarem se a estrutura curricular atual é suficiente para preparar profissionais para os cenários complexos do mundo digital.

5. Conclusões e Trabalhos Futuros

Este trabalho analisou a inserção do tema de Segurança da Informação nas matrizes curriculares dos cursos de Computação de instituições da RFEPCT da Região Sudeste do Brasil. Para isso, investigou-se os PPCs das modalidades bacharelado, licenciatura e tecnologia. Os resultados apontaram uma presença significativa do conteúdo nos cursos de bacharelado e tecnologia. No entanto, observou-se uma baixa inserção nas licenciaturas.

Esse cenário das licenciaturas é bastante crítico, uma vez que a formação de professores sem o devido preparo em Segurança da Informação pode limitar a capacidade de abordar temas fundamentais relacionados à cidadania digital, boas práticas no uso das tecnologias e prevenção de riscos cibernéticos. Tal lacuna tende a fragilizar a formação

de estudantes da educação básica e profissional, contribuindo para um cenário de vulnerabilidade digital ainda maior.

Adicionalmente, a predominância de uma nomenclatura generalista para as disciplinas de segurança, embora garanta a presença do tema, ressalta a necessidade de uma reflexão crítica sobre a profundidade do conteúdo. A efetiva capacitação de profissionais para os desafios atuais depende da incorporação explícita de conceitos como *Security by Design* e da familiaridade com *frameworks* e diretrizes estratégicas da área, como o PPSI do Governo Federal. A ausência de termos-chave nas ementas pode indicar que a abordagem de tópicos essenciais fica a critério do docente, o que sugere a importância de uma estruturação curricular mais robusta e intencional.

Como trabalhos futuros, propõe-se expandir a análise para instituições das demais regiões do país. Além disso, sugere-se realizar uma investigação qualitativa das ementas, a fim de avaliar a profundidade e o escopo da abordagem sobre Segurança da Informação nos cursos analisados, utilizando outras estratégias como entrevistas.

6. Agradecimentos

A revisão textual deste artigo contou com o apoio da ferramenta ChatGPT, desenvolvida pela OpenAI.

Referências

Abu-Taieh, E. M. (2017). Cyber security body of knowledge. In *2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2)*, pages 104–111.

Almohri, H. M., AbuHmed, T., Nyang, D., and Mahmoud, M. (2020). Security-by-design for cyber-physical systems: A survey. *Journal of Systems and Software*, 169:110537.

BRASIL (2023). Programa de privacidade e segurança da informação (ppsi). `https://www.gov.br/governodigital/pt-br/seguranca-da-informacao/programa-de-privacidade-e-seguranca-da-informacao`. Acesso em: 17 mar. 2025.

Bygrave, L. A. (2022). Security by design: Aspirations and realities in a regulatory context. *Oslo Law Review*, 8(3):126–177.

CERT.br (2025). Estatísticas de incidentes - cert.br. `https://stats.cert.br/`. Acesso em: 17 mar. 2025.

CIS (2025). Cis critical security controls v8. `https://www.cisecurity.org/controls/cis-controls-list`. Acesso em: 17 mar. 2025.

CISO Advisor (2024a). Ataque ao santander afeta clientes na espanha, chile e uruguai. `https://shre.ink/MFIU`. Acesso em: 17 mar. 2025.

CISO Advisor (2024b). Ataque na alemanha força até bloqueio de elevadores. `https://www.cisoadvisor.com.br/ataque-na-alemanha-forca-ate-bloqueio-de-elevadores/`. Acesso em: 17 mar. 2025.

Cristani, M., Alves, W., Pereira, G., and Lazarin, N. (2020). Um breve panorama sobre a disciplina de segurança nos cursos de sistemas de informação no brasil. In *Anais*

Estendidos do XVI Simpósio Brasileiro de Sistemas de Informação, pages 1–4, Porto Alegre, RS, Brasil. SBC.

de Barros, J. A. A. (2023). Segurança cibernética nas escolas e universidades brasileiras: avaliando a inserção da educação cibernética no sistema educacional brasileiro e seus efeitos na prevenção de incidentes cibernéticos. Acesso em: 22 mar. 2025.

G1 Mato Grosso do Sul (2023). De cpf a fotos: Ufms confirma que dados pessoais de alunos foram acessados por hackers em vazamento. https://shre.ink/MFIl. Acesso em: 17 mar. 2025.

IBM Security (2023). X-force threat intelligence index 2023. https://www.ibm.com/reports/threat-intelligence. Acesso em: 17 mar. 2025.

Lopes, M. S. S. (2023). Avaliação da estruturação da capacitação na área de segurança cibernética nas instituições e sua contribuição para a evolução do conhecimento em segurança cibernética. Acesso em: 22 mar. 2025.

Marconi, M. d. A. and Lakatos, E. M. (2003). *Fundamentos de metodologia científica*. Atlas, São Paulo, 5 edition.

Ministério da Educação (2016). Resolução cne/ces nº 5, de 16 de novembro de 2016. http://portal.mec.gov.br/index.php?option=com_docman&view=download&alias=52101-rces005-16-pdf&category_slug=novembro-2016-pdf&Itemid=30192. Acesso em: 22 mar. 2025.

Ministério da Educação (2025). Eixo tecnológico: Informação e comunicação - catálogo nacional de cursos superiores de tecnologia. https://cncst.mec.gov.br/eixo-tecnologico?id=5. Acesso em: 20 mar. 2025.

Ministério da Saúde (2022). Ministério da saúde anuncia restabelecimento total dos sistemas afetados por ataque hacker. https://shre.ink/MFIc. Acesso em: 17 mar. 2025.

NIST (2024). The nist cybersecurity framework (csf) 2.0. Technical Report NIST CSWP 29, National Institute of Standards and Technology.

O Globo (2023). Grupos americanos caesars e mgm são vítimas de ataque hacker. https://shre.ink/MFIm. Acesso em: 17 mar. 2025.

Security Leaders (2024). Universidade federal do paraná sofre ataque cibernético. https://securityleaders.com.br/universidade-federal-do-parana-sofre-ataque-cibernetico/. Acesso em: 17 mar. 2025.

Souza, J. G. S., Arima, C. H., and Belda, F. R. (2020). Análise de tratamento da segurança da informação de uma instituição de ensino público federal. *Revista Ibero-Americana de Estudos em Educação*, 15(3):1309–1321.

UFRGS (2024). Universidade de howard é alvo de ataque de ransomware. https://www.ufrgs.br/infabico/universidade-de-howard-e-alvo-de-ataque-de-ransomware/. Acesso em: 17 mar. 2025.

Wazlawick, R. S. (2020). *Metodologia de Pesquisa para Ciência da Computação*. GEN LTC, 3 edition.